STATEMENT OF WORK

For

Air Force Medical Operations Agency (AFMOA)

Medical Device Information Security Support Services
(MDISS)

Solicitation/Contract Number: ID05180035

05 November 2018

TABLE OF CONTENTS

STATEMENT OF WORK (SOW)
Medical Device Information Security Support Services

1.0. DESCRIPTION OF SERVICES

1.1. Background. The mission of the Air Force Medical Operations Agency (AFMOA) is to support development and oversee execution of Air Force Surgeon General Policies in optimizing the health and wellness of our population through appropriate, effective and efficient healthcare practices and service delivery at 76 Medical Treatment Facilities (MTFs) throughout the Continental United States (CONUS), Outside the Continental United States (OCONUS), and deployed locations. AFMOA's Clinical Engineering (CE) Branch provides operational support, analysis, and program management support of both a single MTF and Air Force Medical Service (AFMS) enterprise-level medical device acquisitions, maintenance & support, cybersecurity, facility design, and other related functions.

1.2. Scope. This Statement of Work (SOW) defines the general tasks for non-personal services including management and professional support, studies, analyses, evaluations, engineering and technical services. The contractor shall provide support to AFMOA's CE Branch as it relates to medical device network security, cybersecurity, Information Technology (IT) management and refresh, and medical device deployment management as defined in Air Force Instruction (AFI) 41-209, Medical Logistics Support (AFGM 2015- 01, Air Force Guidance Memorandum to AFI 41-209,Chapter 6.13, Management of Computer and Communications Systems).

1.2.1. The Government will neither supervise Contractor personnel nor control the method by which the Contractor performs the required tasks. Under no circumstances will the Government assign tasks outside the scope of this SOW, or prepare work schedules for Contractor personnel. It shall be the responsibility of the Contractor to manage its personnel and to guard against any actions that are personal services, or give the perception of personal services. If the Contractor feels any actions constitute, or are perceived to constitute personal services, notify the Contracting Officer (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the Contractor shall be the sole responsibility of the Government.

2.0. GENERAL INFORMATION

2.1. Contractor Identification. All Contractor/Subcontractor personnel will identify themselves as Government Contractor personnel during all forms of communications such as business meetings, telephone conversations, electronic mail, attendance sheets, coordination documentations, reports, and the signature blocks utilized in all correspondence. If a contract requires Government workspace, the Contractor/Subcontractor personnel shall wear a picture identification badge and identify their workspace area with their name and company affiliation.

2.2. Contractor Training. Contractor employees are to complete initial, continuing, and refresher cybersecurity training at the awareness level, policy level, implementation level and performance level in accordance with Public Law 100-235; 5 CFR 930.301. Contractors are to

complete mandatory HIPAA and Privacy Act training course within 30 calendar days of on-boarding and obtaining network access and annually, thereafter.

Additionally, Contractor employees are to complete Enterprise Mission Assurance Support Services (eMASS) training or other A&A Tracking Tool identified by Government within 30 calendar days of onboarding and obtaining network access. Throughout the life of the task order, there could be other Government identified training that will require contractor employees to complete. All other training shall be completed within 30 calendar days of onboarding and obtaining network access.

Government will provide information to obtain training and certification to contractor post award.

2.3. Contractor/Government Communication. The Contractor shall designate a Focal Point to be the single point of contact for all Contractor and Government correspondence. The Focal Point shall provide clear and consistent written and verbal response to Government within 12 business hours of Government initiated communication (e.g., return phone calls, emails or other communication). Normal duty hours are annotated in section 2.7 of the SOW.

2.3.1. The Contractor's Focal Point/Program Manager shall be responsible for the oversight and coordination of the performance of work, and have full authority to act for the Contractor on all matters relating to daily operation of the task order. The Contractor's Focal Point/Program Manager shall meet with the Government team at least quarterly. The Government or the Contractor may request additional meetings, as necessary. The Contractor shall provide an agenda and meeting minutes. Agendas and Outlook reminders are sent no later than (NLT) five (5) business days prior to meetings. Meeting minutes are sent NLT two (2) business days following the meeting.

2.3.2. Project Management Plan (PMP): The contractor shall prepare a PMP identifying the type/detail of data needed from the Government developed project milestones. The Government milestones will describe the technical approach, organizational resources, and management controls to be employed to meet the performance and schedule requirements for this effort.

2.3.2.1. The Government Program Manager (GPM) shall receive the revised PMP in electronic form, Microsoft Word. Based on the PMP, the GPM will provide approval to move forward on activities planned. The contractor shall request prior approval on all activities not included in the plan or any modifications to the plan after approval has been given.

2.3.2.2. Draft PMP due five (5) business days after the post award meeting, and provide updates within one (1) business day of project changes. Final PMP due one (1) business day after final approval received by all team personnel, with updates as they occur.

2.3.3. Personnel Retention and Recruitment

The Contractor shall make every effort to retain personnel in order to ensure continuity until task order completion. If it should become necessary to substitute or replace personnel, the Contractor shall immediately notify the GPM and copy the CO and GSA Contracting Officer Representative (COR) in writing of any potential vacancies and shall submit the resume(s) of

replacement personnel within 14 calendar days of the notification. The Contractor shall submit the resume(s) of all potential personnel selected to perform under this contract to the GPM and copy the CO and GSA COR through email, or any other process means identified/required, for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 calendar days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. This may necessitate the use of temporary employees to fill short term gaps between permanently assigned employees. Long-term absences are considered those longer than two weeks in duration.

2.4. Place of Performance. The work to be performed under this task order will be in the Medical Device Information Security (MDIS) Program Management Office (PMO) and the Medical Device Technology (MDT) Program Management Office (PMO) located at Fort Detrick, Maryland.

2.5. Period of Performance. The period of performance will consist of a base period of 1-year with four 1-year option periods.

A 15 calendar day phase-in period for this effort is anticipated and will be included in the base period of 12 months. During the phase-in period, the contractor shall prepare to assume full responsibility for assigned service areas in accordance with the terms and conditions of the task order. The contractor shall take all actions necessary for a smooth transition of task order operations. The contractor shall ensure personnel transition ramp-up; follow all AF processes for obtaining badging, knowledge transfer, phase approach to ownership of on-going tasks without interruption, and system orientation.

2.6. Travel Requirements.

2.6.1. The Contractor shall be required to perform regular travel within the CONUS and OCONUS. Contractor personnel shall have a valid passport for OCONUS travel by the task order start date and maintain a valid passport, at no cost to the Government, for length of contract. Some travel may be required to attend/conduct IA tests, device deployments, conferences, and meetings. Anticipated travel under this task may include Department of Defense (DoD), Defense Health Agency (DHA), Air Force (AF), or vendor sites. Travel must be coordinated and authorized by the GPM (copy the CO and GSA COR) at least 14 business days prior to trip (unless notification was received by GPM or CO after that period) and prior to incurring costs. Contractor costs for travel will be reimbursed in accordance with FAR 31.205-46, in arrears. The travel costs shall be reasonable and allowable as defined in FAR 31.201 and in accordance with the limitations of the JTR.

The contractor shall invoice monthly on the basis of cost incurred. The contractor must provide documentation in support of all travel expenses. The contactor will not be reimbursed for local travel (within a 50-mile radius of the government/contractor's facility) or commuter travel (commute from home to work site).

Invoice submissions including travel costs shall include completed travel expense sheets (i.e., travel voucher) for each trip and each employee who traveled. The travel expense report,

receipts of $75 or more (with exceptions being lodging and transportation), and supporting documentation (e.g., approval email for exceeding per diem rates, cost comparisons, etc.) shall be submitted with the invoice. Expense report(s) must include the traveler's name, dates of travel, destination, purpose of travel, Approval Authority documentation (e.g., copy of the e-mail authorizing travel by Government official), and cost for each trip. All travel costs shall be compiled into the Government provided travel expense sheet (SOW Appendix B) or similar document that has been determined to be acceptable by the Government. The entire submission shall be complete and organized to enable the Government to complete an efficient review. Submissions that are not complete and organized are subject to rejection.

2.6.2. Travel is estimated at least once every six (6) weeks and duration can vary from one (1) to five (5) days. Projected travel is provided as SOW Appendix C.

2.6.3. After each trip, a trip report is required which shall include at a minimum following: dates of travel, destination, purpose, individuals contacted, brief synopsis, issues & challenges, recommendations, and a signature. This report shall go to the GPM and copy the CO and GSA COR. This trip report is separate from the expense report and supporting documentation that is required for travel for invoicing purposes. The contractor shall also save a copy of the trip reports in the designated area of the Government shared drive.

2.7. Mission/Emergency Essential. None of the services listed in this SOW are mission/emergency essential.

2.8. Duty Hours. Normal duty hours will consist of eight hours; 40 hours per week. The core work hours are Monday-Friday, 7:30 am – 4:30 pm. The contractor shall be available during these hours. Any flex to these hours shall be coordinated and approved by the GPM.

2.9. Telework/Telecommuting: Telework/telecommuting is authorized for this SOW on an ad hoc or situational basis in the event of unplanned closure of the facility due to natural disasters, military emergency, Executive Orders issued by the President or severe weather and at the GPM's discretion. The Contractor shall ensure continuity and timeliness in completing tasks while telecommuting. No Secret Internet Protocol Router Network (SIPRNET) task assignments will be issued nor are necessary to be completed while Contractor personnel are telecommuting. The GSA CO or GPM shall have final approval of all telecommute and schedules. These special and emergency accommodations will also apply when traveling Temporary Duty (TDY) to locations that prohibit direct access to base computer systems. A laptop with a Virtual Private Networks (VPN) account and Common Access Card (CAC) accessibility shall also be provided by the GPM in the event telecommuting is authorized.

2.9.1. The Contractor shall establish guidelines for Contractor employees that are authorized to telework/telecommute. Email notifications when logging on for work and a detailed daily report to the Contractor when logging off for the day to ensure the Contractor can account for 8 hours of work or total hours worked. The Contractor shall notify the Government of any connection issues If the contractor has issues connecting to the Virtual Private Network (VPN) or Outlook Web Access (https://web-mech01.mail.mil/my.policy) the contractor is notify the GPM via email regarding connectivity issues.

2.9.2. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contract employees from actually working at an alternate site, when/as appropriate and specifically authorized by the Government. Contractor shall develop telework policies to comply with the following requirements and address at a generic level within their Quality Control Plan. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor's responsibility to ensure the services are performed in accordance with the terms and conditions of the award.

2.9.2.1. The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes reflect the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the quality control plan. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

2.9.2.2. The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

2.10. Federal Holidays. Federal offices are closed on New Year's Day, Dr. Martin Luther King, Jr. Birthday, Presidents Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day. The contractor shall not report to work these days.

2.11. Conduct of Contractor Personnel. The CO or designated Government representative may require the Contractor to remove from the job site Contractor personnel working under this task order. Removal from the job site or dismissal from the premises shall not relieve the Contractor of the task order requirements.

2.11.1. Contractor personnel shall be required to observe all base and facility parking, safety and traffic regulations that apply to all facility employees.

2.12. Procedures for Payment

2.12.1. Invoices are due no later than the 15th calendar day of the month following the reporting period. The contractor shall submit the invoices and supporting documents, through the ASSIST portal simultaneously with the Monthly Status Report (as an acceptance item) to allow the client and the GSA COR to electronically accept and certify services received by the client representative. The Monthly Status Report shall include, but is not limited to, the items identified below:

- Status of tasks, schedules, deliverables. Status of tasks shall include a summary description and schedule of all tasks completed during the reporting period, all tasks currently on-going during the reporting period and all known tasks assigned for future reporting periods.
- Current and cumulative task funding status (labor and travel funding status to be reported separately as required)
- Outstanding issues, and proposed resolution approaches and actions to resolve any outstanding issues.
- Staffing report identifying current staffing roster, all current vacancies, and a record of all staffing departures.

2.12.2. The contractor is authorized to invoice only for the services and travel ordered by GSA and provided in direct support of the task order. Failure to comply with the procedures outlined may result in payment being delayed at no additional cost to the Government.

2.13. Personal Service. The client determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this contract is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal Services Contract". The Contractor agrees that this is a non-personal services contract. The Contractor is not, nor shall it hold itself out, to be an agent or partner of, or joint venture with, the Government. The Contractor agrees that his/her personnel shall neither supervise nor accept supervision from Government employees. The Government will not control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. Additionally, the Contractor shall take the following steps to preclude performing, or perception of performing "Personal Services" as stipulated in FAR 37.114(c).

3.0. TASK ORDER REQUIREMENTS

The contractor shall provide ten (10) full-time equivalents (FTEs) to provide the tasks described herein. Please refer to SOW Appendix D and Tasks 1-3 below for additional information.

3.1. Task 1: Medical Device Cybersecurity Assistance - 5 FTEs

3.1.1. Contractor personnel shall provide management and professional support, studies, analyses, evaluations, engineering and technical services to the MDIS PMO and the MDT PMO within ten (10) business days after task assignment or as agreed upon by the Government Program Manager. Contractor personnel shall provide Certification and Accreditation (C&A), cybersecurity, and lifecycle management guidance for medical devices/systems deployed throughout the AF in accordance with the timelines established within the PMP for each Cybersecurity certification effort.

3.1.2. Coordinate, review, and process documentation in the development of multiple vendor C&A (Risk Management Framework (RMF), Platform Information Technology (PIT), etc.) artifact documentation which are used in the accreditation process. Upload C&A artifact documentation/notes into appropriate tracking tool and Government provided shared drive location. All C&A documentation shall be submitted within three (3) business days of received information from the vendor, MTF, DHA or other AF agencies. Tracking tool template to be provided to the contractor by the MDIS PMO after task order award.

3.1.3. Assists in conducting Independent Verification and Validation (IV&V) of medical devices from various vendors and Original Equipment Manufacturers (OEMs). This includes interpreting results, ensuring proper implementation of controls, ensuring proper configurations, etc.

3.1.4. Updates security documentation related to reaccreditations, annual reviews, accreditation updates, and when configuration changes are made to the device/systems and upload into the Medical Device Information Assurance (IA) tracking tool, Government provided shared drive location, and/or Enterprise Mission Assurance Support Service (eMASS) a cybersecurity management web-based application, NLT three (3) business days after updates are received from the vendor, MTF, DHA or other AF agencies. If no updates were received from the vendor, or Government entity, the Contractor is to verify with vendors, and Government entities and document said actions within tracking tool. Updates will be made, 30 calendar days, of previous entry. The tracking tool template is to be provided to the contractor by the MDIS PMO after task order award. Ensures medical device manufacturers and vendors are aware and informed on properly configured medical device systems based on up-to-date DoD/DHA/AF C&A security policy requirements and guidance.

3.1.5. Provides information to medical device manufacturers and AF/DHA network security teams on proper medical device patch management processes which includes a requirement for vendors to validate patches prior to installation.

3.1.6. The contractor shall update the PMO Leadership via a Weekly Status Report (template to be provided by the respective PMO after task order award). This report shall include a summary of all contractor work performed, travel, system status, and concerns/recommendations for improvements NLT noon local time each Friday (or next business day if Friday is a holiday).

3.1.7. The Contractor, in conjunction with vendors and MTFs, shall maintain the accreditation of systems and ensure that reaccreditations are completed prior to the expiration of a system's accreditation.

3.1.8. The Contractor shall collaborate with vendors and MTFs to complete continuous monitoring requirements, as provided by the Government, of accredited systems and submit to DHA via C&A Tracking Tool on or prior to the 26th of each month for systems accredited under RMF. Additionally, the contractor shall document, the status of the continuous monitoring requirement via the Weekly Status Report.

3.1.9. Assists in responding to USCYBERCOM, DHA and AF taskers that affect AF Medical Devices.

3.1.10. The Contractor shall consult with equipment manufacturers and other DoD agencies to obtain information used to inform and assist the CE and PMO Leadership in producing sound engineering solutions to enhance the security posture of the medical device systems being deployed, to include the following:

3.1.10.1. Conducts research and informs CE & PMO Leadership on upcoming industry changes that will impact the security posture of medical devices in the AF.

3.1.10.2. Submits data calls to MTF to obtain current inventories and new requirements.

3.1.10.3. Provides information and guidance to PMO Team on best method for certifying specific medical devices; providing guidance and assistance to Government decision maker of not certifying a device or waiting until new (more secure) versions of devices are manufactured.

3.1.10.4. Informs and assists the CE Teams and SG Functional Consultant with the development of medical device workload; development of language that addresses Cybersecurity requirements; and development of DoDI, DHA and AF policy/guidance. All documents will be in electronic format and will be uploaded into appropriate folder in the provided shared drive location. All documents will be labeled "DRAFT" until final Government approval is obtained.

3.1.10.5. Provides MTF requested information and assistance services to MDIS PMO Chief and requesting MTF during security audit testing of legacy or newly installed devices/systems, documenting risks associated with the use of the device/system utilizing the Medical Device IA tracking tool and eMASS web-based application.

3.1.10.6. Assists the CE Branch as a functional representative on various committees and Working Groups (WGs), such as: AF PIT WG, Medical Device Interconnection Control Board (MDICB), select commercial manufacturer/DoD partnership groups, and the joint Military Health System (MHS)/Veteran's Administration (VA) Working Groups (WGs) that will directly impact Air Force Medical Devices when requested by the Government. Contractor personnel will not be a voting member as an attendee of these WGs. Specific tasks include:

3.1.10.6.1.Provides guidance to these groups on current and updated C&A, Cybersecurity, network security, etc., as it relates to medical networks, systems, devices and equipment.

3.1.10.6.2.Conducts the administrative functions to include tasking such as: preparing and submitting meeting agendas, documenting meeting minutes, and coordinating meetings to ensure smooth execution of projects. Agendas and Outlook reminders are sent NLT five (5) business days prior to meetings. Meeting minutes are sent NLT two (2) business days following the meeting.

3.1.10.7. Creates briefings for CE Team briefings, conferences, etc., via Government provided templates or otherwise specified.

3.1.10.8. Upon request by Government PM, develops and updates technical documents, and provides in-house training to members of CE Team.

3.1.11. Interfaces with numerous medical user representatives, commercial device manufacturers, the DHA Cybersecurity Division, and in some cases, other agencies with AF, DHA and DoD C&A. These interactions/communications include, taskings such as: cybersecurity risk assessments (RA), tests and evaluations, technology evaluation and integration, network design, network security applications (Public Key Infrastructure [PKI], VPN, firewalls, Intrusion Detection Systems, etc.), IA web site information, research and evaluation on Cybersecurity matters, incident response and reporting, AFMS, MHS, RMF, Command, Control, Communications, and Computer Intelligence Support Plan (C4ISP) security documentation, technical papers, white papers, military staff package preparation, evaluation of applicable standards of The Joint Commission, Health Insurance Portability and Accountability Act (HIPAA), wireless technologies, and privacy issues. In addition, follows up with DHA or other Service Components on any outstanding cybersecurity requests under DHA, AF or other Service's reviews.

3.1.12. Cybersecurity Team Lead

3.1.13. Assists in the day to day operations and questions relating to Cybersecurity processes and effectiveness of the Cybersecurity Team and overall Program Management Office.

3.1.14. Assist in conducting research into emerging technologies and trends, standards and products to support cybersecurity efforts.

3.1.15. Develops measures and metrics to inform program and stakeholders of risk processes, risk authorizations, policies and standards.

3.1.16. Support the Government in implementing corrective actions identified in the POA&Ms are maintained and updated.

3.1.17. Ensure that internal cybersecurity repositories are being maintained and updated for the Medical Device Program Office.

3.1.18. Ensure that all DoD Information System cybersecurity-related documentation is current and accessible to properly authorized individuals.

3.1.19. Support the government in the transitioning of incoming and outgoing of Medical Device Program Office team members.

3.1.19.1. Provide training to new Medical Device Project Managers and ensures team members are registered for the next available training on the DoD C&A repository (i.e. eMASS). Within 30 calendar days of receiving access, all new Medical Device Cybersecurity Analysts are to have completed the aforementioned training.

3.1.20. Ensure that Medical Device Management Analysts are appointed in writing and provide oversight to ensure they are following established Cybersecurity policies and procedures. Appointment letters to be provided to the contractor by the MDIS PMO after task order award.

3.1.21. Assists Government in managing the workload of the Cybersecurity Team and Medical Device PMO, coordinates projects to ensure progress and timely completion of deliverables.

3.1.22. Perform complex Information Assurance engineering and risk management as required on assigned projects.

3.1.23. Provide training to new Medical Device Project Managers and ensure new Medical Device team members are registered for the next available training for DoD C&A repository (i.e. eMASS)

3.1.24. Assist in establishing strong customer relationships with external and internal customers. Collaborate with customer IA management team. Presents to Government Performs manual checks and risk assessments to ensure defense-in-depth security controls have in fact been implemented and in compliance with documented checklists of IA teams' performance. Ensure systems are delivered with the highest degree of quality and security.

3.2. Task 2: Patch Management Analysis – 4 FTEs

3.2.1. Develop and update a standardized medical device patch management processes.

3.2.2. Monitors and follows DoD, DHA, and AF notifications for required medical device software updates and patches throughout the lifecycle of the medical device and implements corrective action as required.

3.2.3. Update and maintain the existing comprehensive tracking mechanism tool in order to track medical device compliance for all required security updates and patches of the current PMO sponsored medical devices. Tracking tool to be provided to the contractor by the MDIS PMO after task order award.

3.2.4. Serves as liaison between CE Teams and medical device manufactures during the manufacture security update and patch validation process of current PMO sponsored medical devices. By the 26th of each month, the contractor is to obtain system scans for each system assigned either from the medical device vendor or the military treatment facility.

3.2.5. Uses Automated Security Clearance Approval Systems (ACAS)/other DoD security scanning software and coordinates with network operations centers to obtain required security scans of assigned medical devices.

3.2.6. Ensures medical device manufacturer validated patches are installed on the associated medical devices. This may be via coordination with manufacture(s) under a support agreement, through an automated patch server, or manual installation.

3.2.7. Reviews medical device scan and patch compliance with the MDIS PMO and coordinates corrective updates with manufacturer and documents resulting corrections within the IA certification documentation within 10 business days.

3.2.8. Manages, maintains, and coordinates the use of software applications and tools that provide automated patching solutions to medical devices used in AF MTFs.

3.2.9. Conducts research, evaluates, and provides recommendations to CE Leadership on acquisition and deployment strategies for automated patching solutions that could be used to increase medical device security patch compliance.

3.2.10. Plan of Action and Milestone (POA&M) monitoring and documenting updates to ensure projected milestones are met or extensions are submitted prior to POA&M item expiration. POA&M Completion dates are to be updated within a 30 days of expiration for each system assigned.

3.2.11. The contractor shall design, develop, maintain, execute, and improve a comprehensive Continuous Monitoring (CM) program based upon Government guidance and direction. Propose additional components and techniques that could be used to proactively detect and prevent malicious activity.

3.2.12. Coordinates/leads kickoff meetings, on-going project planning meetings, deployment meetings, and project closeout meetings (meetings may be via teleconference, video teleconference, or on-site).

3.2.13. Patch Management Team Lead

3.2.13.1. Assists in the day to day operations and effectiveness of the Patch Management Team.

3.2.13.2. Develops measures and metrics to inform program and stakeholders of risk processes, risk authorizations, policies and standards.

3.2.13.3. Support the Government in implementing corrective actions identified in the POA&Ms are maintained and updated.

3.2.13.4. Support the government in the transitioning of incoming and outgoing of Medical Device Program Office team members.

3.2.13.5. The contractor will support the government in managing daily operations of the Medical Device Program Office.

3.2.13.6. Ensure that Medical Device Management Analysts are appointed in writing and provide oversight to ensure they are following established Cybersecurity policies and procedures.

3.2.13.7. Assists Government in managing the workload of the Patch Management Team, coordinates projects to ensure progress and timely completion of deliverables.

3.2.13.8. Perform complex Information Assurance engineering and risk management as required on assigned projects.

3.2.13.9. Provide training to new Medical Device Project Managers and ensure new Medical Device team members are registered for the next available training for DoD C&A repository (i.e. eMASS). Within 30 calendar days of receiving access, all new Medical Device Cybersecurity Analysts are to have completed the stated training.

3.2.13.10. Assist in establishing strong customer relationships with external and internal customers. Collaborate with customer IA management team. Presents to Government Performs manual checks and risk assessments to ensure defense-in-depth security controls have in fact been implemented and in compliance with documented checklists of IA teams' performance. Ensure systems are delivered with the highest degree of quality and security.

3.3. Task 3: Medical Device Management – 1 FTE

3.3.1. Informs and facilitates enterprise medical device acquisitions, managing device deployments, and developing lifecycle management processes for the medical devices utilized at all AF MTFs.

3.3.2. Provides project management for assigned enterprise medical device/IT deployments. Specific tasks include:

3.3.2.1. Conducts pre-deployment site surveys, needs assessments, data calls and documents/recommends upgrades to, replacement of, and needed repairs for assigned medical devices. Ensures all firewall requests are submitted 30 days prior to site surveys.

3.3.2.2. Develops project timelines, documentation, and provides advice and assistance to the CE and AFMS Leadership across the lifecycle of the device/IT deployment projects.

3.3.2.3. Ensures coordination with all parties that will be impacted by the deployments. This will include coordination with the local MTF Leadership, Biomedical Equipment Technicians (BMET), Logistics Flights, Information Services Flights, vendor/manufactures, Network Operations Centers (NOC), etc. Where applicable, the contractor will develop Memorandums of Understating (MOU) or Memorandums of Agreement (MOA) to ensure all concerned parties clearly understand their roles and responsibilities.

3.3.2.4. Coordinates/leads kickoff meetings, on-going project planning meetings, deployment meetings, and project closeout meetings (meetings may be via teleconference, video teleconference, or on-site).

3.3.2.5. Provides guidance and validates the performance of finalized testing of installed systems. This includes any required AT/CUD and IA security testing and that Air Force and local MTF requirements are met.

3.3.2.6. Informs CE and PMO Leadership on design, coordination, integration, and deployment of medical device isolation strategies; such as the Medical Device Enclave (MDE). In addition, the contractor will serve as the liaison between AFMOA/SGME and DHA during the move from the AF network to the DHA's Medical Community of Interest (MedCOI)/DHA medical network.

3.3.2.7. Participates as a functional representative on DoD, DHA, AF, VA committees, WGs, etc that will directly impact Air Force Medical Devices when requested by the Government. This includes, but is not limited to groups addressing IA/Cybersecurity, medical device management, medical device design, and network design.

3.4. Security Requirements

3.4.1. This is a Secret level classification. The Contractor shall possess the appropriate facility clearance (Secret) by the quotation due date. As such, the Contractor shall possess the appropriate facility security clearance (Secret) prior to performing work on a classified Government contract.

3.4.2. List of Contractor Personnel: The Contractor shall maintain a current listing of Contractor personnel. The list shall include Contractor personnel's name, social security number, and level of security clearance. The list shall be validated and signed by the company Facility Security Officer (FSO) and provided to the CO and Information Security Program Manager (ISPM) at each performance site 30 calendar days prior to the service start date. Updated listings shall be provided when Contractor personnel's status or information changes. A Visit Request for all Contractor personnel with security clearances is required to be sent through the Joint Personnel Adjudication System (JPAS), and must be updated at least annually. The Contractor shall notify the (ISPM) at each operating location 30 calendar days before on-base performance of the service. The notification shall include:

3.4.2.1. Name, address, and telephone number of the company key management representatives.

3.4.2.2. The contract number and contracting agency.

3.4.2.3. The highest level of classified information to which employees require access.

3.4.2.4. The location(s) of service performance and future performance, if know.

3.4.2.5. The date service performance begins.

3.4.2.6. Any change to information previously provided under this paragraph.

3.4.3. Local Area Network (LAN). All Contractor employees requiring access to the Government unclassified computer network shall have a valid National Agency Check (NAC) verified through Joint Personnel Adjudication System (JPAS). No Contractor employee will be provided access to unclassified computer network or its inherent capabilities (i.e., internet access, electronic mail, file and print services, etc.) without a valid NAC. The Contractor shall be aware of and abide by all Government regulations concerning the authorized use of the Government's

computer network including the restriction against using the network to recruit Government personnel or advertise job openings.

3.4.4. Disclosure of Information. In the performance of this contract, the Contractor may have access to data and information proprietary to a Government agency or to another Government Contractor, or of such nature that its dissemination or use, other than as specified in this contract, would be illegal or otherwise adverse to the interests of the Government or others. The Contractor and its personnel shall not divulge or release data or information developed or obtained under performance of this contract, except to authorize Government personnel or upon written approval of the CO. The Contractor and its Contractor personnel shall not use, disclose, or reproduce proprietary information bearing a restrictive legend, other than as specified in the contract.

3.4.5. Non-Disclosure Agreement (NDA). All Contractor employees shall sign the non-disclosure statement (provided at Appendix F) prior to beginning of contract performance. The Contractor must then provide a copy of the signed/dated NDA to the GPM, CO, and GSA COR prior to beginning work. (Appendix F).

3.4.6. Security Requirements for Contractor Personnel Requiring Access To Classified Information: Contractor personnel shall have view access and/or be involved in discussions concerning classified information on the SIPRNET. Contractor personnel shall have view access and/or be involved in discussions concerning classified information on the SIPRNET. A Contractor's "Facility Clearance" is required in accordance with DoD 5220.22-M, NISPOM. The Contractor's Facility Security Officer (FSO) is responsible for ensuring that all Contractor personnel assigned to this task order have the appropriate clearance as stated in this SOW. The Contractor shall be responsible for any/all cost associated with Personnel security clearances. The Contractor shall provide personnel with the required clearance at the time of award.

3.4.6.1. A DoD 254, Contract Security Classification Specification is required.

3.4.6.2. All Contractor personnel shall have a Secret Security Clearance and must be able to work in an environment applicable to classified and unclassified DoD information systems. All Contractor personnel shall have view access only to the SIPRNET, and shall access and analyze Official Use Only (FOUO) and Operations Security (OPSEC) required to execute the responsibilities of this task order. This designator is based on the potential for an individual assigned to this position to adversely impact DoD missions or functions. The position categories on this task order include Limited Privileged and Non-Privileged, as defined in DoD 5200.2-R (reference (r)). Investigative requirements for each category vary.

3.4.7. Visitor Group Security Agreement (VGSA): The Contractor shall enter into a long-term visitor group security agreement if service performance is on base. This agreement shall outline how the Contractor integrates security requirements for service operations with the AF to ensure effective and economical operation on the installation. The agreement shall include:

3.4.7.1. Security support provided by the AF to the Contractor shall include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation

of security incidents, base traffic regulations and the use of security forms and conducting inspections required by DoD 5220.22-R, Industrial Security Regulation, Air Force Policy Directive 31-6, Industrial Security, and Air Force Instruction 16-1406, Industrial Security Program Management.

3.4.7.2. Security support requiring joint AF and Contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks and internal security controls for protection of classified material and high-value pilferable property.

3.4.7.3. On base, the long-term visitor group security agreement may take the place of a Standard Practice Procedure (SPP).

3.4.8. Obtaining and Retrieving Identification Media: As prescribed by the AFFAR 5352.242-9000, Contractor access to AF installations, the Contractor shall comply with the following requirements:

3.4.8.1. The Contractor shall obtain base identification for all Contractor personnel who make frequent visits to or perform work on the AF installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished identification badges while visiting or performing work on the installation.

3.4.8.2. No later than three (3) working days prior to contract commencement, the Contractor shall submit a written request on company letterhead to the GPM listing the following: contract number, location of work site, start and stop dates, and names of Contractor employees needing access to the base. The GPM shall endorse the request and forward it to the issuing base pass and registration office or security forces for processing. Contractors shall present Government (state or federal) issued Identification (ID), and U.S. Citizenship and Immigration Services (USCIS) Form I-9, Employment Eligibility Verification, before being issued a pass to enter the installation. Before being issued a pass to enter the installation, a Wants and Warrants check shall be conducted for every individual requesting a pass.

3.4.8.3. The Contractor is responsible for ensuring personnel report to Visitor Reception Center, to present their Form I-9 (Employment Eligibility Verification).

3.4.8.4. Upon completion or termination of the contract or expiration of the identification passes, the Contractor shall ensure that all base identification credentials issued to Contractor personnel are returned to the issuing office. If Contractor personnel have been terminated, the credentials shall be retrieved and returned to issuing activity so these personnel do not have base access. If the credential is not retrieved then Security Forces (SF) shall be notified so base access is not allowed.

3.4.9. Failure to comply with these requirements may result in withholding of final payment.

3.4.10. Pass and Identification Items: The contractor shall ensure the following pass and identification items required for service performance are obtained for personnel.

3.4.10.1. Installation Access Pass (IAP) (DBIDS), Visitor/Vehicle Pass (AFI 31-113), used for contracts for less than six months to include one-day visits (i.e. warranty work).

3.4.10.2. Installation Access Card (IAC) (DBIDS), (AFI 31-113), used for contracts for more than six months or more.

3.4.10.3. DoD CAC, (AFI 36-3026), used for contracts for more than six months and requirement exists for access to the Government computer systems and software. CAC applications are accomplished by Trusted Agents via the Trusted Agent Sponsorship System (TASS).

3.4.11. Entry Procedures to Controlled/Restricted Areas: Contractor personnel requiring unescorted entry to areas designated as controlled or restricted areas by the installation commander shall comply with base access requirements and will possess, as a minimum, a favorable suitability determination. These requirements are contained in AFI 31-101, Integrated Defense, for installation access and AFI 31-501, Personnel Security Program, for suitability determinations. The Contractor shall comply and implement local base procedures for entry to AF controlled/restricted areas. For on-base cleared facilities over-sighted by the base ISPM, Contractors shall comply with the National Industrial Security Program Operating Manual (NISPOM), previously referred to as the Industrial Security Manual (ISM), to implement controlled/restricted area requirements. The ISPM shall approve the establishment, construction, and modification of all Contractor designated controlled areas before they may be used to limit access.

3.4.12. Security Monitor Appointment: The Contractor shall appoint a security representative for the on base long term visitor group. The security representative may be a full-time position or an additional duty position. The security representative shall work with the host organization to provide employees with training required by DoDM 5200.01, Information Security Program, AFPD 31-4, Information Security, and AFI 16-1404 Air Force Information Security Program . The Contractor shall provide initial and follow-on training to Contractor personnel who work in AF controlled/restricted areas. AF restricted and controlled areas are explained in AFI 31-101, Integrated Defense.

3.4.13. Additional Security Requirements: In accordance with DoDM 5200.01, Information Security Program and AFI 16-1404, the Contractor shall comply with AFSSI 7700, Emission Security (EMSEC) Program; applicable AFKAGs, AFIs, and AFSSIs for Communication Security (COMSEC); and AFI 10-701, Operations Security (OPSEC) Instructions. The Contractor will comply with DoD Standard 22/Force Protection Condition Measures, DoD Standard 25/Level I-AT Awareness Training, and associated tasking contained in AFI 10-245, Antiterrorism (AT) standards. Level I AT Awareness training is available, at no cost, for Contractor personnel and can be requested by calling the local installation AT Office.

3.5. Contractor Manpower Reporting Requirements Application (CMRA). The Contractor shall report ALL contractor labor hours (including subcontracted labor hours) required for performance of services provided under this contract for the Air Force and Army via a secure data collection site. The Contractor is required to completely fill in all required data fields at http://www.ecmra.mil. Reporting inputs will be for the labor executed during the period of

performance for each Government fiscal year (FY), which runs 1 October through 30 September. While inputs may be reported at any time during the FY, all data shall be reported no later than 31 October of each calendar year. Contractors may direct questions to the CMRA help desk.

3.6. Uses and Safeguarding of Information. Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any data be released to the public with the Contractor name and contract number associated with the data.

3.7. User Manuals. Data for Air Force service requirements must be input at the Air Force Contract Manpower Reporting Application (CMRA) link. However, user manuals for Government personnel and Contractors are available at the Army CMRA link http://www.ecmra.mil.

3.8. Customer Complaint Record. This form may be utilized by the Government to provide feedback on issues affecting the performance of this task order.

3.9. Meetings.

3.9.1. Post-Award Meeting. The Government will host a post-award meeting with the Contractor within ten (10) business days after contract award. Telecon/teleconference is permissible for the post-award meeting. The purpose of the post-award meeting is introduce the Contractor to the Government representatives (e.g., GPM/CO/GSA COR) the Contractor will support and to ensure a common understanding of the requirements, expectations, and ultimate end products. The Contractor shall discuss the overall understanding of the project and review the background information and materials provided by the Government. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and conducted; assumptions made, expected and results. A concerted effort shall be made to gain a thorough understanding of the client agency expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the Client and the Contractor shall be construed as adding, deleting, or modifying any requirements, including deliverable specifications and due dates.

3.9.2. Initial Contract Performance Review Meeting. The Contractor shall also attend an Initial Contract Performance Review thirty (30) calendar days after the Contractor assumes full performance responsibilities (i.e. after completion of transition/mobilization) to ensure that the Contractor has successfully started performance, completed transition, is fully operational, and is within the estimated schedule and performance parameters of the task order. The Contractor shall also attend a follow-up meeting 90 calendar days after task order award to assess status of performance.

3.10. Applicable Publications. Publications (i.e., certifications, specifications, standards, policies, and procedures) applicable to this requirement include, but are not limited to, those listed in this SOW. The Contractor shall follow all applicable publications and references thereto. Supplements or amendments to listed publications from any organizational level may be issued by the AF Publications Office during the life of the task order. Succeeding revisions may be substituted or incorporated as required with full notice and disclosure to the Contractor. The

Government will provide access to available documents and technical information as required and upon Contractor request for the performance of this task order.

3.10.1. Publications and forms are maintained and available electronically for Contractor download through the internet.

3.10.2. DoD Directives can be found at http://www.dtic.mil/whs/directives/index.html

3.10.3. Regulations are followed by a "---R" (e.g., DoD 6025.18-R) and can be located on the website by clicking on Publications instead of Directives.

3.11. Transition Phase-out Plan. The contractor shall develop a Phase-Out Plan to affect a smooth and orderly transfer of responsibility to a successor contractor and/or Government personnel. This will be provided to the Government for review and acceptance. The Phase-Out Plan shall, at a minimum, establish procedures to implement the handoff, including, but not limited to: an observation period for the incoming workforce to observe operations and performance methods of the incumbent contractor. During phase-out, the incumbent contractor shall not defer any requirements for the purpose of avoiding responsibility or of transferring such responsibility to the succeeding contractor/Government personnel. The incumbent contractor shall fully cooperate with the succeeding contractor and the Government so as not to interfere with their work or duties. The Government anticipates that the last 30 days of the task order will be the phase-in period under the successor task order.

3.12. QUALITY. Both the Contractor and the Government have responsibilities for providing and ensuring quality services, respectively.

3.12.1. Quality Control. The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the requirements of this contract are provided as specified in accordance with the applicable Inspection of Services Clause. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO. The Government has the right to require revisions of the QCP (at no cost to the Government) should the incorporated plan fail to deliver the quality of the services provided at any time during the contract performance. The plan shall include, but is not limited to the following:

- A description of the inspection system covering all services listed.
- The specification of inspection frequency.
- The title of the individual(s) who shall perform the inspection and their organizational placement.
- A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.
- On-site records of all inspections conducted by the Contractor are required. The format of the inspection record shall include, but is not limited to, the following:

- Date, time, and location of the inspection.
- A signature block for the person who performed the inspection.
- Rating of acceptable or unacceptable.
- Area designated for deficiencies noted and corrective action taken.
- Total number of inspections.

3.12.2. Quality Assurance.

The Government will perform periodic reviews of the contractor's performance in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformity with performance and technical requirements.

3.12.3. CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS) Assessment. Upon request by the Government, the contractor shall submit a self-evaluation of their performance at least annually utilizing a Government provided template. From time of Government request, the contractor shall have 9 business days (i.e. initial request due date of 1 week with an additional 2 business day follow-up) to provide input to the GSA COR. The contractor self-assessment will then be submitted to the Government client where they will utilize this information to formulate an independent performance evaluation that will be processed through the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

4.0. SERVICE DELIVERY SUMMARY (SDS)

The following SDS will guide overall performance of this task order. The following criteria will be used to determine if performance requirements are met.

Performance Requirement	Performance Threshold	Acceptable Quality Level (AQL)	Incentive/Disincentive
Task Specific Requirements, Deliverables, and Reporting (reference SOW paragraphs 2.3.1, 2.3.2, and paragraphs and subsequent subparagraphs under 3.1, 3.2, and 3.3)	100% of documentation, reporting, and services shall be completed and submitted IAW the requirements established within the requirement documents (SOW \ work definition \ task directive \ task assignment form, etc.) and shall be compliant with all applicable governing due dates, regulations, policies, directives and guidance. 100% of documentation, reporting, and services shall be completed (including required updates) and submitted NLT the established date for completion/receipt as identified in the requirement documents. Electronic versions of all documentation in the required format shall be posted/stored within the mutually established timeframe in the required artifact repository/tool location and shall be available for Government review at all times as required.	No more than 5 violations per month for each Task. A violation is an omission or delayed delivery.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $5,000.00.

Inquiry Response	Respond to all DHA, Service Components inquiries NLT 3 business days of receipt unless on Leave or TDY then within 3 business days of returning to the office. Respond to all other Government inquiries within time specified by the Government and/or the SOW.	No more than 5 violations per month. A violation is an error delayed response.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 2% up to the maximum reduction of $2,500.00.
Monthly Invoice	100% complete with all required supplemental information. 100% accurate. Submitted no later than (NLT) 15th calendar day of month following the reporting period and submitted concurrent with the monthly status report.	No violations per month. A violation is an error (including grammatical errors), omission, or delayed delivery.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $1,500.00.
Mandatory Government Training Compliance	100% of the training (for all contractor personnel performing under the task order) shall be completed and submitted NLT the established date for training completion as mandated by the Government.	No violations per month.	CPARS assessment ratings.

Personnel Staffing and Retention	100% compliance with staffing requirements identified in SOW paragraph 2.3.3 and paragraph 3 and all subparagraphs.	Ensure qualified staffing and retention is maintained at 90% annually or better throughout the life of the task order. Position shall not be vacant for longer than 2 weeks to include vacations or illnesses.	CPARS assessment ratings. Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $5,000.00.

5.0. GOVERNMENT FURNISHED PROPERTY (GFP)

5.1. The Government will provide the Contractor with the facilities, equipment, and information necessary to perform the tasks stipulated in this task order. Facilities include office space in both classified and unclassified work areas. Equipment includes computers (classified and unclassified), desks, chairs, access to printers, unclassified and classified networks, copy machines, classified destruction equipment, telephones (secure, DSN, commercial access capabilities), basic office supplies, and Government vehicles, if necessary and available. These items are incidental to the place of performance and remain accountable to the Government. In addition, the Government shall require each individual Contractor employee to sign hand receipts for all Information Technology Equipment (ITE) that they exclusively use (i.e., all equipment on their desks). This includes laptops for travel or out-of-office use. Contractor employees are not required to sign for multiple users ITE such as network equipment, network printers, and servers. Information includes all reference material or documentation required to perform. All facilities, equipment, and information used by the Contractor will remain the property of the Government and the Contractor shall return all facilities, equipment, and information to the COR or other designated representative upon the request of the Government or at the end of the task order period of performance.

5.2. When a task order requires the Contractor to work in a Government facility, the Government will furnish or make available working space, equipment and network access. Copies of required materials cited in the task order will be provided to the Contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the COR or other designated representative upon request or at the end of the task order period of performance. Available GFP and facilities will be identified in the SOW. The Contractor's responsibilities for the GFP are outlined in the Government Property clause**.**

6.0. DELIVERABLES

6.1. The Contractor shall submit all deliverables as specified in this SOW.

6.2. All deliverables must be submitted electronically to the GPM, unless otherwise identified below. All deliverables must be submitted electronically to the GPM using standard Microsoft Office products (e.g., Word, Excel, PowerPoint, Access etc.)

6.3. The GPM may approve extensions to the delivery timeline based on magnitude and complexity of the document topic.

6.4. Provide informal reports by e-mail, as requested by the GPM.

Deliverable Title	SOW Paragraph/Section	Format	Delivery Due Date
Contractor Employee Training Certifications	2.2	Electronic Certification/Certificate via applicable training website.	HIPAA and Privacy Act training course within 30 calendar days of on-boarding and obtaining network access and annually, thereafter. Enterprise Mission Assurance Support Services (eMASS) training within 30 calendar days of onboarding and obtaining network access. Other Government identified training within 30 calendar days of onboarding and obtaining network access.
Quarterly Feedback Meetings - Agenda and Minutes	2.3.1	Contractor Format	Agendas and Outlook reminders are sent NLT five (5) business days prior to meetings. Meeting minutes are sent NLT two (2)

			business days following the meeting.
Project Management Plan	2.3.2.	Contractor Format, Word	Draft PMP due 5 business days after post-award meeting with all updates due within 1 business day of project changes. Final PMP due 1 business day after final approval received by all team personnel with updates due within 1 business day of change.
Trip Report	2.6.3	Government provided template, Word	Within 3 business days from return date. Please copy CO/GSA COR on all email traffic/documentation.
Telework/telecommuting Reporting (if approved by GPM)	2.9.1	Contractor Format, Email	If approved for telework/telecommuting, contractor employees shall send email to notify the Contractor with log-on email and provide daily report detailing actions taken that day when logging off.
Invoice with supporting documentation and Monthly Status Report	2.6 (if travel costs being submitted) & 2.12.1	Contractor Format, via ASSIST/ITSS	NLT 15th calendar day of the month following the reporting period. Submit via ASSIST/ITSS.
Weekly Status Report	3.1.6 & 3.1.8	Government provided template (to be provided after award)	NLT noon local time each Friday (or next business day if Friday is a holiday)
RMF Reporting	3.1.8	Government provided and submitted via C&A Tracking Tool	NLT 26th of each month for systems accredited under RMF
Other Meetings (as needed) – Agenda and Minutes	3.1.10.6.2		Agendas and Outlook reminders are sent NLT five (5) business

		Contractor Format	days prior to meetings. Meeting minutes are sent NLT two (2) business days following the meeting
Conferences/Briefings	3.1.11.7	Government provided templates or otherwise specified	As tasked by the Government.
Medical Device Management Analysts Appointment Letters	3.1.20	Government provided template	After award but prior to commencement of performance by Contractor personnel.
Tracking Mechanism Tool	3.2.3	Government provided document	As tasked by the Government.
Contractor Employee Non-disclosure Agreement	3.4.5	Government provided template (SOW Appendix F)	After award but prior to commencement of performance by Contractor personnel. Please copy CO/GSA COR on all email traffic/documentation.
Transition Phase-out Plan	3.11	Contractor Format	NLT 120 calendar days prior to task order completion date. Please copy CO/GSA COR on all email traffic/documentation.

7. APPENDICES

Appendix A – Acronyms and Definitions

Appendix B – Travel Expense Sheet (Template/Sample)

Appendix C – Projected Travel Requirements

Appendix D – MDISS Project Team Structure

Appendix E - Business Associate Agreement

Appendix F - Non-Disclosure Agreement

Appendix A – Acronyms and Definitions

Acronyms and Definitions	
ACRONYM	DEFINITIONS
AT/CUD	Acceptance Testing/Clinical Use Determination
ACAS	Automated Security Clearance Approval System
AF	Air Force
AFI	Air Force Instruction
AFMS	Air Force Medical Service
AFMOA	Air Force Medical Operations Agency
AFMSA	Air Force Medical Support Agency
AIS	Automated Information System
ADP	Automated Data Processing
CAC	Common Access Card
CDRL	Contract Data Requirements List
CE	Clinical Engineering
CONUS	Continental United States
CO	Contracting Officer
COR	Contracting Officer Representative
CPAR	Contractor Performance Assessment Reports
CUD	Clinical Use Determination
DHA	Defense Health Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DoDI	Department of Defense Instructions
DSA	Data Service Agreement
DUA	Data Use Agreement
E/APL	Evaluated/Approved Product List
FAR	Federal Acquisition Regulation
eMASS	Enterprise Mission Assurance Support Service
FDA	Federal Drug Administration
FOUO	For Official Use Only
FTEs	Full Time Equivalent
HIPAA	Health Insurance Portability and Accountability Act of 1996
IA	Information Assurance
IAW	In Accordance With
IT	Information Technology
IV&V	Independent Verification and Validation
JKO	Joint Knowledge Online
MDIS PMO	Medical Device Information Security Program Management Office
MDT	Medical Device Technology
MHS	Military Health System
MTF	Medical Treatment Facility
NACI	National Agency Check and Inquiries
NACLC	National Agency Check with Local Agency Check and Credit Check
NDA	Non-Disclosure Agreement
NLT	No later than
OCONUS	Outside the Continental United States
OCI	Organizational Conflict of Interest
OEM	Original Equipment Manufacturer
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager

PMO	Program Management Office
PMP	Project Management Professional
POC	Point of Contact
QC	Quality Control
QCP	Quality Control Plan
RMF	Risk Management Framework
SGALE	Surgeon General Administration Logistics Engineering
SLA	Service Level Agreement
SORNS	System of Record Notices
SOW	Statement of Work
TDY	Temporary Duty
USCYBERCOM	United States Cyber Command
VA	Veteran's Administration
VPN	Virtual Private Network
VGSA	Visitor Group Security Agreement
WG	Working Group

Appendix B – Travel Expense Sheet (Template/Sample)

PWS Appendix B -
Travel Expense Sheet

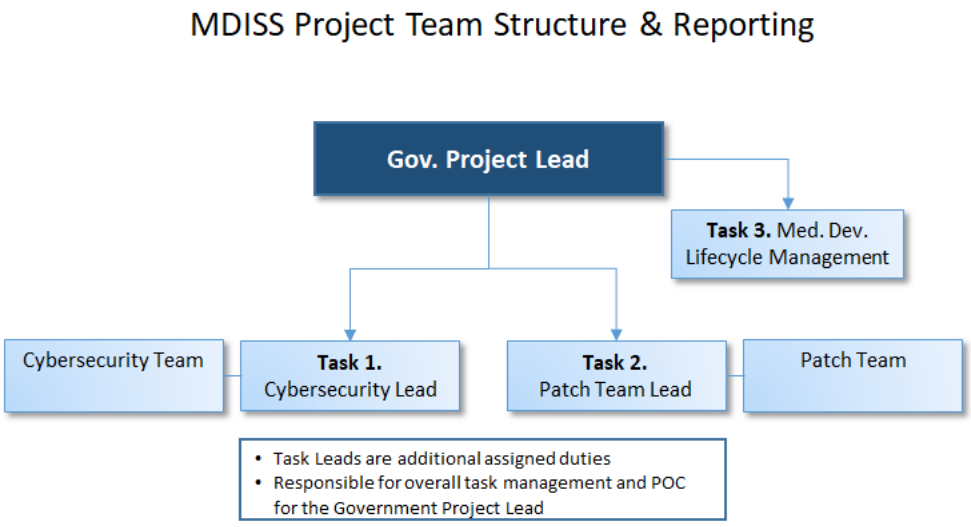
Appendix C – Projected Travel Requirements

Projected Travel Requirements				
Trip Purpose	**Projected Dates of Travel**	**Travel Location From/To**	**No. of Trip Days**	**No. of Travelers**
RSNA Vendor Meetings to discuss new medical device technology, patch management, scanning, etc. Annual meeting that Branch members attend. Saves multiple trips to vendor sites.	11/25/18 - 11/30/18	RSNA Meetings Chicago, IL (Westermann)	6	2
Cybersecurity Testing		MRS IV&V Lackland AFB, TX (Kenneth Y.)	5	1
Cybersecurity Testing		AGFA IDC IV&V Scott AFB (Tom W.)	5	1
Cybersecurity Testing		AGFA NX IV&V Greenville, SC (Bill F.)	5	1
Cybersecurity Testing		ScriptCenter IV&V San Diego, CA (Tom L.)	5	1
Cybersecurity Testing		DIMS IV&V Andover, MA (Chris)	5	1
Cybersecurity Testing		Fuji CVIS IV&V Wright-Patterson AFB, OH (Tom W.)	5	1
Cybersecurity Testing		GE Revolution IV&V Shaw AFB, SC (Bill F.)	5	1
Cybersecurity Testing		Epiphany IV&V Elmendorf AFB, AK (Tom W.)	5	1
HIMSS Vendor Meetings to discuss new medical systems technologies, patch management, scanning, etc. Annual meeting that Branch members attend. Saves multiple trips to vendor sites.		HIMSS Meetings Orlando (Legg or Alt Analyst)	5	1
Same as above, but HIMSS pays for Erich registrations saving AF $695-$895.)		HIMSS Meetings Orlando (Bill)	5	1
Cybersecurity Testing for one of our systems; there are many in the works and specifics noted herein and estimating more projects will make it through this stage. Cost estimates based on average of known sites.		IV&V TBD	5	1
		IV&V TBD	5	1
		IV&V TBD	5	1
		IV&V TBD	5	1
N/A		Travis Pharmacy Will Call Install and Acceptance Testing (Erich)	5	1
N/A		Lackland Will Call Install and Acceptance Testing (Erich)	5	1
N/A		Wright-Patterson Will Call Install and Acceptance Testing (Erich)	5	1
Working Contracts and expect to happen FY 19. Cost estimates based on average of known sites.		Will Call Install and Acceptance Testing	5	1

		TBD (Erich)		
		Will Call Install and Acceptance Testing TBD (Erich)	5	1
Site order may move around, but installs will take place. Used average CONUS/OCONUS cost estimates. Trips include acceptance testing, cybersecurity updates (OS, etc.) of new Pharmacy Systems.		CONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		CONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		CONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		CONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		CONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		OCONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		OCONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
		OCONUS Innovation Pharmacy Upgrades and Windows 10 Compliance (Erich)	5	1
This is the main joint federal pharmacy meeting; discussions and meetings with key pharmacy vendors, service consultants, integration experts (GENISIS), etc.		Joint Federal Pharmacy Seminar-Location TBD (Erich)	5	1
This is board certification committee for systems personnel across the AFMS. Supports DHA and AFMS missions by providing primary board certification process for officer and enlisted personnel. HIMSS & ACHE pays for most of Cost.		HIMSS & ACHE Exam Committee Meeting Chicago, IL-x3 (Erich)	5	1
Site order may move around, but installs will take place. Used average CONUS/OCONUS cost estimates. Trips include acceptance testing, cybersecurity updates (OS, etc.) of new Pharmacy Systems.		CONUS ES Pharmacy Install (Erich)	5	1
		CONUS ES Pharmacy Install (Erich)	5	1
		CONUS ES Pharmacy Install (Erich)	5	1
		CONUS ES Pharmacy Install (Erich)	5	1
		CONUS ES Pharmacy	5	1

		Install (Erich)		
		CONUS ES Pharmacy Install (Erich)	5	1
		OCONUS ES Pharmacy Install (Erich)	6	1
		OCONUS ES Pharmacy Install HI (Erich)	6	1
		OCONUS ES Pharmacy Install AK (Erich)	6	1
		OCONUS ES Pharmacy Install GE (Erich)	6	1
		OCONUS ES Pharmacy Install UK (Erich)	6	1

Appendix D – MDISS Project Team Structure



Appendix E - Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This BAA can serve as a separate standalone agreement or may be used for new or existing contracts between the MTF and the business associate.

Business Associate Agreement

[**USE FOR STANDALONE BAA ONLY**] This Business Associate Agreement (this "Agreement") is entered into this ___ day of _____, _____ (the "Effective Date") between [**NAME OF MHS COVERED ENTITY**] ("Covered Entity") and [**NAME OF BUSINESS ASSOCIATE**], a [type of business entity] ("Business Associate").

Introduction

In accordance with 45 CFR 164.502(e)(2) and 164.504(e) and paragraph C.3.4.1.3 of DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003, this document serves as a business associate agreement (BAA) between the signatory parties for purposes of the Health Insurance Portability and Accountability Act (HIPAA) and the "HITECH Act" amendments thereof, as implemented by the HIPAA Rules and DoD HIPAA Issuances (both defined below). The parties are a DoD Military Health System (MHS) component, acting as a HIPAA covered entity, and a DoD contractor, acting as a HIPAA business associate. The HIPAA Rules require BAAs between covered entities and business associates. Implementing this BAA requirement, the applicable DoD HIPAA Issuance (DoD 6025.18-R, paragraph C3.4.1.3) provides that requirements applicable to business associates must be incorporated (or incorporated by reference) into the contract or agreement between the parties.

(a) Catchall Definition. Except as provided otherwise in this BAA, the following terms used in this BAA shall have the same meaning as those terms in the DoD HIPAA Rules: Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices (NoPP), Protected Health Information (PHI), Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Breach means actual or possible loss of control, unauthorized disclosure of or unauthorized access to PHI or other Personally Identifiable Information (PII) (which may include, but is not limited to PHI), where persons other than authorized users gain access or potential access to such information for any purpose other than authorized purposes, where one or more individuals will be adversely affected. The foregoing definition is based on the definition of breach in DoD Privacy Act Issuances as defined herein.

Business Associate shall generally have the same meaning as the term "business associate" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean [**INSERT NAME OF BUSINESS ASSOCIATE**].

Agreement means this BAA together with the documents and/or other arrangements under which the Business Associate signatory performs services involving access to PHI on behalf of the MHS component signatory to this BAA.

Covered Entity shall generally have the same meaning as the term "covered entity" in the DoD HIPAA Issuances, and in reference to this BAA, shall mean [**INSERT NAME OF MTF COMPONENT**].

DHA Privacy Office means the DHA Privacy and Civil Liberties Office. The DHA Privacy Office Director is the HIPAA Privacy and Security Officer for DHA, including the National Capital Region Medical Directorate (NCRMD).

DoD HIPAA Issuances means the DoD issuances implementing the HIPAA Rules in the DoD Military Health System (MHS). These issuances are DoD 6025.18-R (2003), DoDI 6025.18 (2009), and DoD 8580.02-R (2007).

DoD Privacy Act Issuances means the DoD issuances implementing the Privacy Act, which are DoDD 5400.11 (2007) and DoD 5400.11-R (2007).

HHS Breach means a breach that satisfies the HIPAA Breach Rule definition of breach in 45 CFR 164.402.

HIPAA Rules means, collectively, the HIPAA Privacy, Security, Breach and Enforcement Rules, issued by the U.S. Department of Health and Human Services (HHS) and codified at 45 CFR Part 160 and Part 164, Subpart E (Privacy), Subpart C (Security), Subpart D (Breach) and Part 160, Subparts C-D (Enforcement), as amended by the 2013 modifications to those Rules, implementing the "HITECH Act" provisions of Pub. L. 111-5. See 78 FR 5566-5702 (Jan. 25, 2013) (with corrections at 78 FR 32464 (June 7, 2013)). Additional HIPAA rules regarding electronic transactions and code sets (45 CFR Part 162) are not addressed in this BAA and are not included in the term HIPAA Rules.

Service-Level Privacy Office means one or more offices within the military services (Army, Navy, or Air Force) with oversight authority over Privacy Act and/or HIPAA privacy compliance.

I. Obligations and Activities of Business Associate

(a) The Business Associate shall not use or disclose Personal Health Information (PHI) other than as permitted or required by this Agreement or as required by law.

(b) The Business Associate shall use appropriate safeguards, and comply with the DoD HIPAA Rules with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by this Agreement.

(c) The Business Associate shall report to Covered Entity any Breach of which it becomes aware, and shall proceed with breach response steps as required by Part V of this BAA. With respect to electronic PHI, the Business Associate shall also respond to any security incident of which it becomes aware in accordance with any Information Assurance provisions of this Agreement. If at any point the Business Associate becomes aware that a security incident involves a Breach, the Business Associate shall immediately initiate breach response as required by part V of this BAA.

(d) In accordance with 45 CFR 164.502(e)(1)(ii)) and 164.308(b)(2), respectively, and corresponding DoD HIPAA Issuances, as applicable, the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such PHI.

(e) The Business Associate shall make available PHI in a Designated Record Set, to the Covered Entity or, as directed by the Covered Entity, to an Individual, as necessary to satisfy the Covered Entity obligations under 45 CFR 164.524 and corresponding DoD HIPAA Issuances.

(f) The Business Associate shall make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526, and corresponding DoD HIPAA Issuances.

(g) The Business Associate shall maintain and make available the information required to provide an accounting of disclosures to the Covered Entity or an individual as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.528 and corresponding DoD HIPAA Issuances.

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the HIPAA Privacy Rule, the Business Associate shall comply with the requirements of the HIPAA Privacy Rule that apply to the Covered Entity in the performance of such obligation(s); and

(i) The Business Associate shall make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

II. Permitted Uses and Disclosures by Business Associate

(a) The Business Associate may only use or disclose PHI as necessary to perform the services set forth in this Agreement or as required by law. The Business Associate is not permitted to de-identify PHI under DoD HIPAA issuances or the corresponding 45 CFR 164.514(a)-(c), nor is it permitted to use or disclose de-identified PHI, except as provided by this Agreement or directed by the Covered Entity **[MODIFY THIS SECTION IF THE PURPOSE OF THE AGREEMENT/CONTRACT IS FOR THE BA TO DEIDENTIFY PHI FOR THE CE]**.

(b) The Business Associate agrees to use, disclose and request PHI only in accordance with the HIPAA Privacy Rule "minimum necessary" standard and corresponding DHA policies and procedures as stated in the DoD HIPAA Issuances.

(c) The Business Associate shall not use or disclose PHI in a manner that would violate the DoD HIPAA Issuances or HIPAA Privacy Rules if done by the Covered Entity, except uses and disclosures for the Business Associate's own management and administration and legal responsibilities or for data aggregation services as set forth in the following three paragraphs.

(d) Except as otherwise limited in this Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. The foregoing authority to use PHI does not apply to disclosure of PHI, which is covered in the next paragraph.

(e) Except as otherwise limited in this Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(f) Except as otherwise limited in this Agreement, the Business Associate may use PHI to provide Data Aggregation services relating to the Covered Entity's health care operations.

III. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) The Covered Entity shall notify the Business Associate of any limitation(s) in the notice of privacy practices of the Covered Entity under 45 CFR 164.520 and the corresponding provision of the DoD HIPAA Issuances, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) The Covered Entity shall notify the Business Associate of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes affect the Business Associate's use or disclosure of PHI.

(c) The Covered Entity shall notify the Business Associate of any restriction on the use or disclosure of PHI that the Covered Entity has agreed to or is required to abide by under 45 CFR 164.522 and the corresponding DoD HIPAA Issuances, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.

IV. Permissible Requests by Covered Entity

The Covered Entity shall not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule or any applicable Government regulations (including without limitation, DoD HIPAA Issuances) if done by the Covered Entity, except for providing Data Aggregation services to the Covered Entity and for management and administrative activities of the Business Associate as otherwise permitted by this BAA.

V. Breach Response

(a) In general.

(1) In the event of a breach of PII/PHI held by the Business Associate, the Business Associate shall report the breach to the Covered Entity in accordance with Section VII, assess the breach incident, take mitigation actions as applicable, and notify affected individuals, as directed by the Covered Entity.

(2) The Business Associate shall coordinate all investigation actions with the Covered Entity, and at a minimum, follow the breach response requirements set forth in this Part V, which is designed to satisfy both the Privacy Act and HIPAA as applicable. If a breach involves PII without PHI, then the Business Associate shall comply with DoD Privacy Act Issuance breach response requirements only; if a breach involves PHI (a subset of PII), then the Business Associate shall comply with both Privacy Act and HIPAA breach response requirements. A breach involving PHI may or may not constitute an HHS Breach. If a breach is not an HHS Breach, then the Business Associate has no HIPAA breach response obligations. In such cases, the Business Associate must still comply with breach response requirements under the DoD Privacy Act Issuances.

(3) The Business Associate shall, at no cost to the government, bear any costs associated with a breach of PII/PHI that the Business Associate has caused or is otherwise responsible for addressing.

(b) Government Reporting Provisions

(1) If the Covered Entity determines that a breach is an HHS Breach, then the Business Associate shall comply with both the HIPAA Breach Rule and DoD Privacy Act Issuances, as directed by the Covered Entity, regardless of where the breach occurs. If the Covered Entity determines that the breach does not constitute an HHS Breach, then the Business Associate shall comply with DoD Privacy Act Issuances, as directed by the applicable Service-Level Privacy Office.

(2) This Part V is designed to satisfy the DoD Privacy Act Issuances and the HIPAA Breach Rule as implemented by the DoD HIPAA Issuances. In general, for breach response, the Business Associate shall report the breach to the Covered Entity, assess the breach incident, notify affected individuals, and take mitigation actions as applicable. Because DoD defines “breach” to include possible (suspected) as well as actual (confirmed) breaches, the Business Associate shall implement these breach response requirements immediately upon the Business Associate’s discovery of a possible breach.

(3) The following provisions of Part V set forth the Business Associate’s Privacy Act and HIPAA breach response requirements for all breaches, including but not limited to HHS breaches.

(i) The Business Associate shall report the breach within one hour of discovery to the US Computer Emergency Readiness Team (US CERT), and, within 24 hours of discovery, to the Covered Entity, and to other parties as deemed appropriate by the Covered Entity. The Business Associate is deemed to have discovered a breach as of the time a breach (suspected or confirmed) is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing it) who is an employee, officer or other agent of the Business Associate.

(ii) The Business Associate shall submit the US-CERT report using the online form at https://forms.us-cert.gov/report/. Before submission to US-CERT, the Business Associate shall save a copy of the on-line report. After submission, the Business Associate shall record the US-CERT Reporting Number. Although only limited information about the breach may be available as of the one hour deadline for submission, the Business Associate shall submit the US-CERT report by the deadline. The Business Associate shall e-mail updated information as it is obtained, following the instructions at http://www.us-cert.gov/pgp/email.html. The Business Associate shall provide a copy of the initial or updated US-CERT report to the Installation Privacy Act Officer, MTF HIPAA Privacy Officer, and the Contracting Officer (if applicable), if requested. Business Associate questions about US-CERT reporting shall be directed to the Installation Privacy Act Officer or MTF HIPAA Privacy Officer, not the US-CERT office.

(iii) The Business Associate shall comply with the Breach Timeline and Notification Flow Chart processes attached to this Agreement, to include the timelines established for completing the DD Form 2959 and the HIPAA Privacy Incident Report.

(4) If multiple beneficiaries are affected by a single event or related set of events, then a single reportable breach may be deemed to have occurred, depending on the circumstances. The Business Associate shall inform the Covered Entity as soon as possible if it believes that "single event" breach response is appropriate; the Covered Entity will determine how the Business Associate shall proceed and, if appropriate, consolidate separately reported breaches for purposes of Business Associate report updates, beneficiary notification, and mitigation.

(i) When a Breach Report Form initially submitted is incomplete or incorrect due to unavailable information, or when significant developments require an update, the Business Associate shall submit a revised form or forms, stating the updated status and previous report date(s) and showing any revisions or additions in red text. Examples of updated information the Business Associate shall report include, but are not limited to: confirmation on the exact data elements involved, the root cause of the incident, and any mitigation actions to include, sanctions, training, incident containment, and follow-up. The Business Associate shall submit these report updates within three (3) business days after the new information becomes available. Prompt reporting of updates is required to allow the Covered Entity to make timely final determinations on any subsequent notifications or reports. The Business Associate shall provide updates to the same parties as required for the initial Breach Reporting Form. The Business Associate is responsible for reporting all information needed by the Covered Entity to make timely and accurate determinations on reports to HHS as required by the HHS Breach Rule and reports to the Defense Privacy and Civil Liberties Office as required by DoD Privacy Act Issuances.

(ii) In the event the Business Associate is uncertain on how to apply the above requirements, the Business Associate shall consult with the **Covered Entity and Contracting Officer** (if applicable) when determinations on applying the above requirements are needed.

(c) Individual Notification Provisions

(i) If the Covered Entity determines that individual notification is required, the Business Associate shall provide written notification to individuals affected by the breach as soon as possible, but no later than 10 working days after the breach is discovered and the identities of the individuals are ascertained. The 10 day period begins when the Business Associate is able to determine the identities (including addresses) of the individuals whose records were impacted.

(ii) The Business Associate's proposed notification to be issued to the affected individuals shall be submitted to the parties to which reports are submitted under paragraph VII for their review, and for approval by the [**REMOVE CO REFERENCES FOR STAND-ALONE AGMT**] **Contracting Officer, in consultation with the** Covered Entity. Upon request, the Business Associate shall provide the **Contracting officer and** Covered Entity with the final text of the notification letter sent to the affected individuals. If different groups of affected individuals receive different notification letters, then the Business Associate shall provide the text of the letter for each group (PII shall not be included with the text of the letter(s) provided). Copies of further correspondence with affected individuals need not be provided unless requested by the **Contracting Office or** Covered Entity. The Business Associate's notification to the individuals, at a minimum, shall include the following:

(A) The individual(s) must be advised of what specific data was involved. It is insufficient to simply state that PII has been lost. Where names, Social Security Numbers (SSNs) or truncated SSNs, and Dates of Birth (DOBs) are involved, it is critical to advise the individual that these data elements potentially have been breached.

(B) The individual(s) must be informed of the facts and circumstances surrounding the breach. The description should be sufficiently detailed so the individual clearly understands how the breach occurred.

(C) The individual(s) must be informed of what protective actions the Business Associate is taking or the individual can take to mitigate against potential future harm. The notice must refer the individual to the current Federal Trade

Commission (FTC) web site pages on identity theft and the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

(F) The individual(s) must also be informed of any mitigation support services (e.g., one year of free credit monitoring, identification of fraud expense coverage for affected individuals, provision of credit freezes, etc.) the Business Associate may offer affected individuals, the process to follow to obtain those services and the period of time the services will be made available, and contact information (including a phone number, either direct or toll-free, e-mail address and postal address) for obtaining more information. The [**REMOVE CO REFERENCES FOR STAND-ALONE AGMT**] **Contracting Officer, in consultation with the** Covered Entity will determine the appropriate level of support services.

(iii) Business Associates shall ensure any envelope containing written notifications to affected individuals are clearly labeled to alert the recipient to the importance of its contents, e.g., "Important information – do not destroy," and the envelope is marked with the identity of the Business Associate and/or subcontractor organization that suffered the breach. The letter must also include contact information for a designated POC to include, phone number, e-mail address, and postal address.

(iv) If the Business Associate determines that it cannot readily identify, or will be unable to reach, some affected individuals within the 10 day period after discovering the breach, the Business Associate shall so indicate in the initial or updated Breach Report Form. Within the 10 day period, the Business Associate shall provide the approved notification to those individuals who can be reached. Other individuals must be notified within 10 days after their identities and addresses are ascertained. The Business Associate shall consult with the Covered Entity, which will determine which media notice is most likely to reach the population not otherwise identified or reached. The Business Associate shall issue a generalized media notice(s) to that population in accordance with the Covered Entity approval.

(d) Breaches are not to be confused with security incidents (often referred to as cyber security incidents when electronic information is involved), which may or may not involve a breach of PII/PHI. In the event of a security incident not involving a PII/PHI breach, the Business Associate shall follow applicable DoD Information Assurance requirements under its Agreement. If at any point the Business Associate finds that a cybersecurity incident involves a PII/PHI breach (suspected or confirmed), the Business Associate shall immediately initiate the breach response procedures set forth here. The Business Associate shall also continue to follow any required cyber security incident response procedures to the extent needed to address security issues, as determined by DoD/DHA.

VI. Termination

(a) Termination. Noncompliance by the Business Associate (or any of its staff, agents, or subcontractors) with any requirement in this BAA may subject the Business Associate to termination under any applicable default or other termination provision of **the underlying Contract** [**FOR STANDALONE INSERT, REPLACE WITH** "**this Agreement**"].

(b) Effect of Termination.

(1) If this Agreement has records management requirements, the Business Associate shall handle such records in accordance with the records management requirements. If this Agreement does not have records management requirements, the records should be handled in accordance with paragraphs VI.(2) and (3) below. If this Agreement has provisions for transfer of records and PII/PHI to a successor Business Associate, or if the Covered Entity gives directions for such transfer, the Business Associate shall handle such records and information in accordance with such Agreement provisions or the Covered Entity's direction.

(2) If this Agreement does not have records management requirements, except as provided in the following paragraph (3), upon termination of this Agreement, for any reason, the Business Associate shall return or destroy all PHI received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall retain no copies of the PHI.

(3) If this Agreement does not have records management provisions and the Business Associate determines that returning or destroying the PHI is infeasible, the Business Associate shall provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Covered Entity and the Business Associate that return or destruction of PHI is infeasible, the Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such PHI.

VII. Notices. Any notices to be given hereunder will be made in the most expedient manner, via e-mail, facsimile, U.S. Mail, or express courier to such party's address given below.

If to the Business Associate:		If to the Covered Entity:	
Attn:		Attn:	
Title:		Title:	MTF HIPAA Privacy Officer
Company:		Unit:	
Address:		Address:	
Phone:		Phone:	
Fax:		Fax:	
E-mail:		E-mail:	

With a copy to:

Name:		Name:	
Company:		Title:	Contracting Officer
Address:		Address:	

Phone:		Phone:	
Fax:		Fax:	
Email:		Email:	

Each party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner provided in this subsection.

VIII. Miscellaneous

(a) Survival. The obligations of Business Associate under the "Effect of Termination" provision of this BAA shall survive the termination of this Agreement.

(b) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity and the Business Associate to comply with the HIPAA Rules and the DoD HIPAA

[**USE FOR STANDALONE BAA ONLY**] (c) Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. The parties acknowledge and agree that faxed and/or electronically affixed signatures shall act as original signatures that bind each faxing, or electronically affixing, signatory to the terms and provisions of this Agreement. Delivery of an executed counterpart of this Agreement by facsimile or electronic mail shall be equally effective as delivery of a manually executed counterpart.

[**USE FOR STANDALONE BAA ONLY**] (d) Entire Agreement; Amendment. This Agreement embodies the entire understanding between the parties pertaining to the subject matter contained in it; supersedes any and all prior negotiations, correspondence, understandings, or agreements of the parties with respect to its subject matter; and may be waived, altered, amended, modified, revised or repealed, in whole or in part, only on the written consent of the parties to this Agreement.

[**USE FOR STANDALONE BAA ONLY**] IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

[**USE FOR STANDALONE BAA ONLY**]

BUSINESS ASSOCIATE:		**COVERED ENTITY:**	
Signature:		Signature:	
Print name:		Print name:	
Title:		Title:	

Date: Date:

Appendix F – Non-Disclosure Agreement

HQ USAF/SG NON-DISCLOSURE AGREEMENT
REVISED: 30 AUG 2007

Purpose: The purpose of this Non-Disclosure Agreement (NDA) is to confirm in writing that the undersigned understands his/her responsibilities regarding protection of information and/or material that he/she may come in contact with in the course of work performed under this agreement. This NDA covers all forms of information made available as Government Furnished Information or information/material developed under this agreement, whether in the form of working materials or as deliverable product. This NDA applies to unclassified Government information/material, proprietary information/material supplied by other vendors for use by the Government, and classified Government information/material and is intended to supplement, not replace, the DD Form 254. All information/material released to the contractor remains the property of the US Government and may be withdrawn at any time.

Responsibility: As a condition of acceptability for work under this agreement with Air Force Material Command /773 ESS/PK on behalf of AF/SG, individuals are required to complete the attached NDA:

(Continued)
NON-DISCLOSURE AGREEMENT FOR CONTRACTOR/SUBCONTRACTOR EMPLOYEES, SENIOR MANAGERS OR CORPORATE OFFICERS

I, _____ (clearly print or type name), an employee, senior manager, or corporate officer of either _____ or a subcontractor to _____ under Prime Contract number _____; Task Order _____ awarded to _____ by the AF/SG office (Customer) agree not to disclose to any third party or anyone who is not performing work for the Customer and who does not have a need to know such information, any proprietary, source selection sensitive information, programmatic, or budgetary information (Information) contained in or accessible through the AF/SG programs and activities. Proprietary, programmatic, budgetary and source selection sensitive information and data will be handled in accordance with Government direction under the AF/SG program and applicable Government laws and regulations, including Federal Acquisition Regulation (FAR) Sections 3.104 and 9.5.

I understand that Information I may receive or possess, as a result of my assignment to work on AF/SG activities under this Contract may be considered proprietary, source selection sensitive information, and/or For Official Use Only. The responsibilities of my employer for the proper use and protection from unauthorized disclosure of proprietary or source selection sensitive information are described in FAR 3.104. Pursuant to FAR 3.104, I agree that I shall not appropriate such information for my own use or release or discuss such information with third parties unless specifically authorized by the procedures set forth in FAR 3.104.

This Agreement shall continue for a term of five (5) years from the date upon which I last have access to such information. Upon expiration of this Agreement, I have a continuing obligation not to disclose proprietary, programmatic, budgetary or source selection sensitive information to any person or legal entity unless that person or legal entity is authorized by the Government to receive such Information. I understand that any violation of my duty to protect proprietary or source selection sensitive information I was exposed to while working as an employee of _____ company working under the Prime Contract, subcontract, or task order as referenced above may subject me, and/or my employer, to administrative, civil and criminal sanctions.

I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement. Court costs and reasonable attorney fees incurred by the United States Government may be assessed against me if I lose such action. I understand that another company might file a separate claim against me if I have misused its proprietary information.

In the event that I seek other employment, I will reveal to any prospective employer the continuing obligation in this agreement prior to accepting any employment offer.

If signing as a corporate officer of either the Prime or Subcontractor, I certify that I am a duly authorized representative with legal authority to bind the Company.

Agreed and Accepted:

_____

(Signature of Employee) (Date)

_____

(Printed Name/Position) (Telephone Number)

_____

(Signature of Employer Sr. Mgr/Officer) (Date)

_____

(Printed Name/Position) (Telephone Number)